UNITED STATES DISTRICT COURT
DISTRICT OF RHODE ISLAND

HAYLEY BOURQUE and ALLISON DURR, on behalf of themselves and all others similarly situated, Plaintiffs, v. NAUTIC PARTNERS, LLC, Defendant.	Case No.: 1:24-CV-00047-MSM-LDA **AMENDED CLASS ACTION COMPLAINT** **JURY TRIAL DEMAND**

Hayley Bourque and Allison Durr ("Plaintiffs"), through their attorneys, on behalf of themselves and all others similarly situated, bring this Amended Class Action Complaint against Defendant Nautic Partners, LLC ("Nautic" or "Defendant"), and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities. Plaintiffs allege the following on information and belief—except as to their own actions, counsel's investigations, and facts of public record.

NATURE OF ACTION

1. This class action arises from Defendant's failure to protect highly sensitive data.

2. Defendant is a private equity firm that specializes in healthcare, outsourcing services, and industrial products.[1] And Defendant advertises that it "has managed over $9.5 billion in assets since its founding in 1986."[2]

3. As such, Defendant stores a litany of highly sensitive personal identifiable information ("PII") and protected health information ("PHI")—together "PII/PHI"—about its

[1] *Home Page*, NAUTIC, https://nautic.com/ (last visited Jan. 23, 2024).
[2] *Id*.

current and former employees and/or customers. But Defendant lost control over that data when cybercriminals infiltrated its insufficiently protected computer systems in a data breach (the "Data Breach").

4. It is unknown for precisely how long the cybercriminals had access to Defendant's network before the breach was discovered. In other words, Defendant had no effective means to prevent, detect, stop, or mitigate breaches of its systems—thereby allowing cybercriminals unrestricted access to its current and former employees' and/or customers' PII/PHI.

5. On information and belief, cybercriminals were able to breach Defendant's systems because Defendant failed to adequately train its employees on cybersecurity and failed to maintain reasonable security safeguards or protocols to protect the Class's PII/PHI. In short, Defendant's failures placed the Class's PII/PHI in a vulnerable position—rendering them easy targets for cybercriminals.

6. Plaintiffs are Data Breach victims, having received breach notices—attached as Exhibit A. They bring this class action on behalf of themselves, and all others harmed by Defendant's misconduct.

7. The exposure of one's PII/PHI to cybercriminals is a bell that cannot be unrung. Before this data breach, its current and former employees' and/or customers' private information was exactly that—private. Not anymore. Now, their private information is forever exposed and unsecure.

PARTIES

8. Plaintiff Hayley Bourque is a natural person and citizen of Massachusetts. She resides in Melrose, Massachusetts, where she intends to remain.

9. Plaintiff, Allison Durr, is a natural person and citizen of New York. She resides in Armonk, New York where she intends to remain.

10. Defendant, Nautic Partners, LLC, is a Foreign Limited Liability Company incorporated in Delaware and with its principal place of business at 50 Kennedy Plaza, 17th Floor Providence, Rhode Island 02903.

JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Plaintiffs and Defendant are citizens of different states. And there are over 100 putative Class members.

12. This Court has personal jurisdiction over Defendant because it is headquartered in Rhode Island, regularly conducts business in Rhode Island, and has sufficient minimum contacts in Rhode Island.

13. Venue is proper in this Court because Defendant's principal office is in this District, and because a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in this District.

BACKGROUND

Defendant Collected and Stored the PII/PHI of Plaintiffs and the Class

14. Defendant is a private equity firm that specializes in healthcare, outsourcing services, and industrial products.[3] And Defendant advertises that it "has managed over $9.5 billion in assets since its founding in 1986."[4]

[3] *Home Page*, NAUTIC, https://nautic.com/ (last visited Jan. 23, 2024).
[4] *Id*.

15. As part of its business, Defendant receives and maintains the PII/PHI of thousands of its current and former employees and/or customers.

16. In collecting and maintaining the PII/PHI, Defendant agreed it would safeguard the data in accordance with its internal policies, state law, and federal law. After all, Plaintiffs and Class members themselves took reasonable steps to secure their PII/PHI.

17. Under state and federal law, businesses like Defendant have duties to protect its current and former employees' and/or customers' PII/PHI and to notify them about breaches.

18. Defendant recognizes these duties, declaring in its "Privacy Policy" that:

a. "Your privacy is important to Nautic Partners, LLC and its affiliates."[5]

b. "This Website Privacy Policy (this 'Privacy Policy'), which is supplemented by the California Website Privacy Supplement and the EU and UK Website Privacy Supplement (each, a 'Supplement' and together, the 'Supplements'), describes how we gather and use personally identifiable information, personal information, personal data or other similar terms under applicable data protection and privacy laws, including, as applicable, the GDPR and CCPA (as defined below), ('PII') for visitors of the Site (as defined below)."[6]

c. "This Privacy Policy, and each Supplement, is being provided to inform you of our practices for collecting, using, maintaining, protecting, and disclosing PII that we obtain from you: . . . through offline and online

[5] *Privacy Policy*, NAUTIC, https://nautic.com/privacy-policy/ (last visited Jan. 23, 2024).
[6] *Id*.

communications (including emails) . . . when you visit our offices . . . to conduct business with you . . . [and] when you apply for a job with us[.]"

d. "We are committed to protecting the PII you entrust to us."[7]

e. "We implement security measures designed to protect any PII submitted by or collected from you from unauthorized access."[8]

f. "We further protect your PII from potential security breaches by implementing certain technological security measures in accordance with generally accepted industry practices."[9]

g. "In addition, we limit access to your PII to those employees, agents, contractors and other third parties who have a business need to know. They will only process your PII on our instructions and they are subject to a duty of confidentiality."[10]

h. "We will retain PII we collect from you, and PII you provide to us, in connection with our internal record-keeping policies, including as reasonably necessary to comply with our legal obligations and regulatory requirements, resolve disputes, prevent fraud or abuse and enforce our Privacy Policy and Terms of Use. We will not keep more information than we need for those purposes."[11]

i. "We consider the protection of sensitive information to be a sound business practice, and to that end we employ appropriate organizational, physical,

---

[7] *Id.*
[8] *Id.*
[9] *Id.*
[10] *Id.*
[11] *Id.*

technical and procedural safeguards, which seek to protect your PII in our possession or under our control to the extent possible from unauthorized access and improper use."[12]

j. "We will not disclose any PII about you to anyone, except as permitted or required by law or regulation, to service providers and as set out in the relevant Supplement."[13]

19. Likewise, via its "ESG" webpage, Defendant declares that: "Nautic seeks to ensure that appropriate data governance standards and procedures are implemented both internally and at our portfolio companies to comply with regulatory standards and safeguard sensitive data, including proprietary portfolio company intellectual property, from malicious actors."[14]

Defendant's Data Breach

20. In early 2023, Defendant was hacked.[15] However, the precise timeframe of the Data Breach is unclear.

21. Thus far, Defendant has been less than forthcoming—only explaining that "[w]e discovered unauthorized access to our network occurred between February 23, 2023 and April 5, 2023."[16]

22. Thus, it is unclear if the Data Breach spanned the entire 41 days between February 23 and April 5.

---

[12] *Id*.
[13] *Id*.
[14] *ESG*, NAUTIC, https://nautic.com/firm/esg/ (last visited Jan. 23, 2024).
[15] *Data Breach Notifications*, MAINE ATTY GEN, https://apps.web.maine.gov/online/aeviewer/ME/40/570e5c34-bdb2-46f1-af58-cd73c90eabc1.shtml (last visited Jan. 23, 2024).
[16] *Id*.

23. In total, Defendant injured at least 7,870 persons—via the exposure of their PII/PHI—in the Data Breach.[17]

24. Defendant has not explained its relationship to the 7,870 persons that it exposed.[18] Thus, upon information and belief, these 7,870 persons include Defendant's current and former employees and/or customers.

25. Because of Defendant's Data Breach, at least the following types of PII/PHI were compromised:

a. names;

b. Social Security numbers;

c. driver's license numbers;

d. government-issued ID numbers;

e. passport numbers;

f. state ID cards;

g. financial information;

h. financial account numbers;

i. credit card numbers;

j. debit card numbers; and

k. medical records.[19]

---

[17] *Id*.
[18] *See id*.
[19] *Data Security Breach Reports*, ATTY GEN TEXAS, https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage (last visited Jan. 23, 2024); *Data Breach Notification Report*, OFF. CONSUM. AFFS & BUS. REG., https://www.mass.gov/doc/data-breach-report-2024/download (last visited Jan. 23, 2024).

26. And yet, Defendant waited until January 12, 2024, before it began notifying the class—a ***full 323 days*** after the Data Breach began.[20]

27. Thus, Defendant kept the Class in the dark—thereby depriving the Class of the opportunity to try and mitigate their injuries in a timely manner.

28. And when Defendant did notify Plaintiffs and the Class of the Data Breach, Defendant acknowledged that the Data Breach created a present, continuing, and significant risk of suffering identity theft, warning Plaintiffs and the Class:

a. "[W]e encourage you to take [steps] to protect yourself against misuse of your personal information."[21]

b. "[R]emain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis."

c. "[W]e recommend that you contact your financial institution to inquire about steps to take to protect your account, including whether you should close your account or obtain a new account number."[22]

d. "Review your 'explanation of benefits statement' which you receive from your health insurance company."[23]

e. "Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation

[20] *Data Breach Notifications*, MAINE ATTY GEN, https://apps.web.maine.gov/online/aeviewer/ME/40/570e5c34-bdb2-46f1-af58-cd73c90eabc1.shtml (last visited Jan. 23, 2024).
[21] *Id*.
[22] *Id*.
[23] *Id*.

of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date."[24]

f. "Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize."[25]

29. Defendant failed its duties when its inadequate security practices caused the Data Breach. In other words, Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII/PHI. And thus, Defendant caused widespread injury and monetary damages.

30. Since the breach, Defendant has promise to "continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information."[26]

31. But this is too little too late. Simply put, these measures—which Defendant now recognizes as necessary—should have been implemented *before* the Data Breach.

32. On information and belief, Defendant failed to adequately train its employees on reasonable cybersecurity protocols or implement reasonable security measures.

33. Further, the Notice of Data Breach shows that Defendant cannot—or will not—determine the full scope of the Data Breach, as Defendant has been unable to determine precisely what information was stolen and when.

34. Defendant has done little to remedy its Data Breach. True, Defendant has offered some victims credit monitoring and identity related services. But upon information and belief, such

---

[24] *Id.*
[25] *Id.*
[26] *Id.*

services are wholly insufficient to compensate Plaintiffs and Class members for the injuries that Defendant inflicted upon them.

35. Because of Defendant's Data Breach, the sensitive PII/PHI of Plaintiffs and Class members was placed into the hands of cybercriminals—inflicting numerous injuries and significant damages upon Plaintiffs and Class members.

36. Moreover, this Data Breach reveals a *pattern* of negligent data security by Defendant. After all, this Data Breach is Defendant's second in recent years.

37. Specifically, "[o]n February 11, 2022, an unauthorized third party gained access to the Nautic Partners, LLC ('Nautic') Microsoft O365 environment."[27] Defendant explained that:

a. "Once inside the environment, the Threat Actor sent out phishing emails from the impacted O365 account in an attempt to compromise additional organizations."[28]

b. "The data that was subject to unauthorized access may have contained names and dates of birth, Social Security numbers, financial account, credit card and debit card numbers, and protected health information."[29]

38. Worryingly, the cybercriminals that obtained Plaintiffs' and Class members' PII/PHI appear to be the notorious cybercriminal group known as "LockBit."[30]

---

[27] *Notice of Data Breach*, MASS ATTY GEN, https://www.mass.gov/doc/assigned-data-breach-number-27850-nautic-partners-llc/download (last visited Jan. 23, 2024).
[28] *Id*.
[29] *Id*.
[30] *Nautic Partners*, BREACHSENSE, https://www.breachsense.com/breaches/nautic-partners-data-breach/ (last visited Jan. 23, 2024); *see also Lockbit3*, RANSOMLOOK, https://www.ransomlook.io/group/lockbit3 (last visited Jan. 23, 2024).

39. Arising in Russia during early 2020, "LockBit" is now "the most deployed ransomware variant across the world and continues to be prolific in 2023."[31]

40. Thus, the Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), the Multi-State Information Sharing and Analysis Center (MS-ISAC) have warned that:

a. "LockBit affiliates have employed double extortion by first encrypting victim data and then exfiltrating that data while threatening to post that stolen data on leak sites."[32]

b. "Up to the Q1 2023, a total of 1,653 alleged victims were observed [i.e., published] on LockBit leak sites."[33]

41. And Reuters reports that:

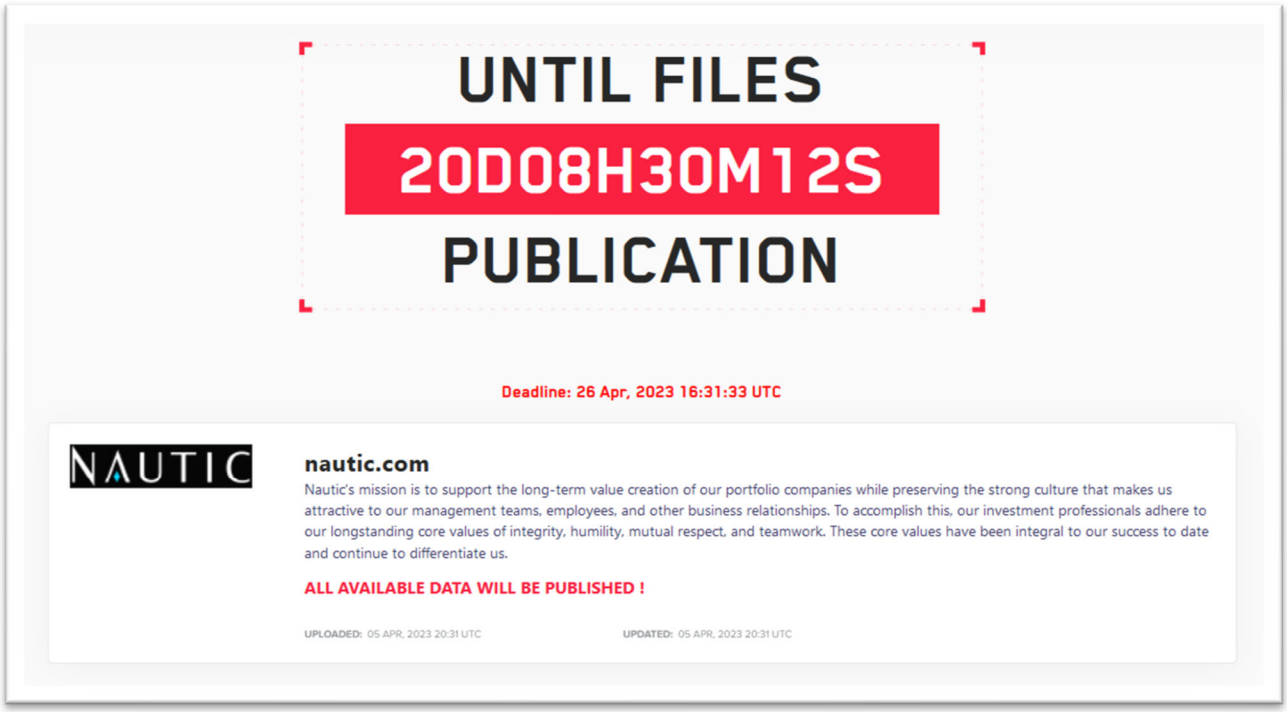
a. "On the dark web, Lockbit's blog displays an ever-growing gallery of victim organisations that is updated nearly daily."[34]

b. "Next to their names are digital clocks showing the number of days left to the deadline given to each organisation to provide ransom payment, failing which, the gang publishes the sensitive data it has collected."[35]

---

[31] *Cybersecurity Advisory*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (June 14, 2023) https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a.
[32] *Id*.
[33] *Id*.
[34] Zeba Siddiqui & James Pearson, *Explainer: What is Lockbit? The digital extortion gang on a cybercrime spree*, REUTERS (Nov. 10, 2023) https://www.reuters.com/technology/cybersecurity/what-is-lockbit-digital-extortion-gang-cybercrime-spree-2023-11-10/.
[35] *Id*.

42. Worryingly, it appears that LockBit already published the stolen PII/PHI—after all, the cybercriminal group indicated that it would publish the stolen PII/PHI on the Dark Web on April 26, 2023.[36]



43. Thus, on information and belief, Plaintiffs' and the Class's stolen PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

Plaintiff Bourque's Experience

44. Plaintiff Hayley Bourque does not know how or when Defendant obtained her PII, and she was not familiar with Defendant before receiving the Notice Letter. However, upon information and belief, the precise connection between Plaintiff Bourque and Defendant can be ascertained from information within Defendant's possession, custody, and/or control.

[36] Vishwa Pandagle, *LockBit Ransomware Group Claims Nautic Cyberattack*, CYBER EXPRESS (April 6, 2023) https://thecyberexpress.com/nautic-cyberattack-lockbit-ransomware-breach/.

45. At the time of the Data Breach—February 23, 2023 through April 5, 2023—Defendant retained Plaintiff Bourque's PII in its system.

46. Plaintiff Bourque is very careful about sharing her sensitive PII. Plaintiff stores any documents containing her PII in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff would not have entrusted her PII to Defendant had she known of Defendant's lax data security policies.

47. Plaintiff Bourque received the Notice Letter, by mail, from Defendant, dated January 12, 2024. According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties, including her name and Social Security number.

48. While Ms. Bourque's Notice Letter does not mention specifically mention compromised financial information, financial account numbers, credit card numbers, and debit card numbers, she has a good faith belief that her financial account and debit card numbers were compromised in this Data Breach, arising from Defendant's disclosures to states' attorneys general (like the Massachusetts AG) that such information was included in this Data Breach.[37]

49. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, which instructs Plaintiff Bourque to "remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis[,]"[38] Plaintiff Bourque made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching and verifying the legitimacy of the Data Breach, contacting Defendant to obtain more details about the Data Breach and how Defendant came into possession of her PII,

[37] *Notice of Data Breach*, Mass Atty Gen, https://www.mass.gov/doc/assigned-data-breach-number-27850-nautic-partners-llc/download (last visited Jan. 23, 2024).

[38] Notice Letter

contacting financial institutions to sort out fraudulent activity on her accounts, visiting government offices to sort out fraudulent activity on her accounts, replacing impacted debit cards, and securing her financial accounts. Plaintiff Bourque has spent significant time on mitigation activities in response to the breach—valuable time Plaintiff Bourque otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

50. Plaintiff Bourque suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) statutory damages; (vii) nominal damages; and (vii) the continued and certainly increased risk to her PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

51. Plaintiff Bourque also suffered actual injury in the form of experiencing multiple fraudulent charges to her Eastern Bank debit card, for nearly $1000, in or about March 2023, which, upon information and belief, was caused by the Data Breach.

52. Plaintiff Bourque also suffered actual injury in the form of experiencing multiple fraudulent charges to her Food Stamp, for approximately $400, in or about March 2023, which, upon information and belief, was caused by the Data Breach.

53. It is well known that stolen Social Security numbers can be used to commit food stamp fraud, as is the case with Plaintiff Bourque. Prominent websites such as Wikihow

specifically note that "[a] person with a stolen Social Security Number may be using it to obtain food stamps," and provide instructions on what to do if one's Social Security number is used for that improper purpose.[39]

54. Plaintiff Bourque further suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails that occurred after this Data Breach and which, upon information and belief, were caused by the Data Breach.

55. The Data Breach has caused Plaintiff Bourque to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed her of key details about the Data Breach's occurrence. As a result of the Data Breach, Plaintiff Bourque anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

56. As a result of the Data Breach, Plaintiff Bourque is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

57. Plaintiff Bourque has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Durr's Experiences and Injuries

58. To the best of her ability, Plaintiff Allison Durr is unsure how Defendant came to obtain—and thus ultimately expose—her highly sensitive PII/PHI.

[39] See https://www.wikihow.life/Report-Someone-Using-a-Stolen-SSN (last visited April 15, 2024)

59. Nonetheless, Plaintiff Allison Durr received a data breach notice from Defendant explaining to her that her PII/PHI was exposed in its Data Breach. As such, Plaintiff was injured by Defendant's Data Breach.

60. Upon information and belief, Defendant obtained Plaintiff Durr's PII/PHI pursuant to its business operations—e.g., pursuant to an employee-employer relationship, a patient-provider relationship, and/or a business relationship.

61. Upon information and belief, the precise connection between Plaintiff Durr and Defendant can be ascertained from information within Defendant's possession, custody, and/or control.

62. As a condition of her (or her third-party agent's) employment and/or other relationship with Defendant, Plaintiff Durr (or her third-party agent) provided Defendant with Plaintiff's PII/PHI. Defendant then used that PII/PHI to facilitate its business.

63. Plaintiff Durr (or her third-party agent) provided her PII/PHI to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff's PII/PHI and has a continuing legal duty and obligation to protect that PII/PHI from unauthorized access and disclosure.

64. Plaintiff Durr (or her third-party agent) reasonably understood that a portion of the funds paid to Defendant (and/or derived from employment) would be used to pay for adequate cybersecurity and protection of PII/PHI.

65. Plaintiff Durr does not recall ever learning that her information was compromised in a data breach incident—other than the breach at issue here.

66. Plaintiff Durr received a Notice of Data Breach on January 20, 2024.

67. Thus, on information and belief, Plaintiff Durr's PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

68. Through its Data Breach, Defendant compromised Plaintiff Durr's full name and Social Security number.

69. Plaintiff Durr has spent—and will continue to spend—significant time and effort monitoring her accounts to protect herself from identity theft. After all, Defendant directed Plaintiff to take those steps in its breach notice.

70. And in the aftermath of the Data Breach, Plaintiff has suffered from a spike in spam and scam calls, including scams about, *inter alia*:

a. car warranties;

b. extended warranties; and

c. a scam call purporting to be from Experian about a loan that Plaintiff Durr supposedly qualified for because of a data breach.

71. Once an individual's PII is for sale and access on the dark web, as Plaintiff's PII is here as a result of the breach, cybercriminals are able to use the stolen information to gather and steal even more information.[40] On information and belief, Plaintiff Durr's phone number was compromised as a result of the Data Breach.

72. Plaintiff Durr fears for her personal financial security and worries about what information was exposed in the Data Breach.

73. Because of Defendant's Data Breach, Plaintiff Durr has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go

[40] What do Hackers do with Stolen Information, Aura, https://www.aura.com/learn/what-do-hackers-do-with-stolen-information (last visited April 8, 2024).

far beyond allegations of mere worry or inconvenience. Rather, Plaintiff Durr's injuries are precisely the type of injuries that the law contemplates and addresses.

74. Plaintiff Durr suffered actual injury from the exposure and theft of her PII/PHI—which violates her rights to privacy.

75. Plaintiff Durr suffered actual injury in the form of damages to and diminution in the value of her PII/PHI. After all, PII/PHI is a form of intangible property—property that Defendant was required to adequately protect.

76. Plaintiff Durr suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff's PII/PHI right in the hands of criminals.

77. Because of the Data Breach, Plaintiff Durr anticipates spending considerable amounts of time and money to try and mitigate her injuries.

78. Today, Plaintiff Durr has a continuing interest in ensuring that her PII/PHI—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

Plaintiffs and the Proposed Class Face Significant Risk of Continued Identity Theft

79. Because of Defendant's failure to prevent the Data Breach, Plaintiffs and Class members suffered—and will continue to suffer—damages. These damages include, *inter alia*, monetary losses, lost time, anxiety, and emotional distress. Also, they suffered or are at an increased risk of suffering:

a. loss of the opportunity to control how their PII/PHI is used;

b. diminution in value of their PII/PHI;

c. compromise and continuing publication of their PII/PHI;

d. out-of-pocket costs from trying to prevent, detect, and recovery from identity theft and fraud;

e. lost opportunity costs and wages from spending time trying to mitigate the fallout of the Data Breach by, *inter alia*, preventing, detecting, contesting, and recovering from identify theft and fraud;

f. delay in receipt of tax refund monies;

g. unauthorized use of their stolen PII/PHI; and

h. continued risk to their PII/PHI—which remains in Defendant's possession—and is thus as risk for futures breaches so long as Defendant fails to take appropriate measures to protect the PII/PHI.

80. Stolen PII/PHI is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII/PHI can be worth up to $1,000.00 depending on the type of information obtained.

81. The value of Plaintiffs' and Class's PII/PHI on the black market is considerable. Stolen PII/PHI trades on the black market for years. And criminals frequently post and sell stolen information openly and directly on the "Dark Web"—further exposing the information. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[41]

[41] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/

82. For example, PII can be sold at a price ranging from $40 to $200.[42] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[43]

83. It can take victims years to discover such identity theft and fraud. This gives criminals plenty of time to sell the PII/PHI far and wide.

84. One way that criminals profit from stolen PII/PHI is by creating comprehensive dossiers on individuals called "Fullz" packages. These dossiers are both shockingly accurate and comprehensive. Criminals create them by cross-referencing and combining two sources of data—first the stolen PII/PHI, and second, unregulated data found elsewhere on the internet (like phone numbers, emails, addresses, etc.).

85. The development of "Fullz" packages means that the PII/PHI exposed in the Data Breach can easily be linked to data of Plaintiffs and the Class that is available on the internet.

86. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII/PHI stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and Class members, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs' and other Class members' stolen PII/PHI is being misused, and that such misuse is fairly traceable to the Data Breach.

87. Of course, a stolen Social Security number – standing alone – can be used to wreak untold havoc upon a victim's personal and financial life. The popular person privacy and credit

---

[42] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/

[43] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/

monitoring service LifeLock by Norton notes "Five Malicious Ways a Thief Can Use Your Social Security Number," including 1) Financial Identity Theft that includes "false applications for loans, credit cards or bank accounts in your name or withdraw money from your accounts, and which can encompass credit card fraud, bank fraud, computer fraud, wire fraud, mail fraud and employment fraud; 2) Government Identity Theft, including tax refund fraud; 3) Criminal Identity Theft, which involves using someone's stolen Social Security number as a "get out of jail free card;" 4) Medical Identity Theft, and 5) Utility Fraud.[44]

88. It is little wonder that courts have dubbed a stolen Social Security number as the "gold standard" for identity theft and fraud.

89. Defendant disclosed the PII/PHI of Plaintiffs and Class members for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII/PHI of Plaintiffs and Class members to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII/PHI.

90. Defendant's failure to promptly and properly notify Plaintiffs and Class members of the Data Breach exacerbated Plaintiffs and Class members' injury by depriving them of the earliest ability to take appropriate measures to protect their PII/PHI and take other necessary steps to mitigate the harm caused by the Data Breach.

[44] https://lifelock.norton.com/learn/identity-theft-resources/kinds-of-id-theft-using-social-security-number (last visited April 15, 2024)

Defendant Knew—Or Should Have Known—of the Risk of a Data Breach

91. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in recent years.

92. In 2023, an all-time high for data compromises occurred, with 3,205 compromises affecting 353,027,892 total victims.[45] Of the 3,205 recorded data compromises, 809 of them, or 25.2% were in the medical or healthcare industry.[46] The estimated number of organizations impacted by data compromises has increased by +2,600 percentage points since 2018, and the estimated number of victims has increased by +1400 percentage points.[47] The 2023 compromises represent a 78 percentage point increase over the previous year and a 72 percentage point hike from the previous all-time high number of compromises (1,860) set in 2021.[48]

93. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service issue warnings to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[49]

---

[45] *See 2023 Data Breach Annual Report*, IDENTITY THEFT RESOURCE CENTER (Jan. 2024); https://www.idtheftcenter.org/wp-content/uploads/2024/01/ITRC_2023-Annual-Data-Breach-Report.pdf .

[46] *Id*.

[47] *Id.*

[48] *Id*.

[49] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.

94. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[50]

95. In the third quarter of the 2023 fiscal year alone, 7333 organizations experienced data breaches, resulting in 66,658,764 individuals' personal information being compromised.[51]

96. As a custodian of PII, Defendant knew, or should have known, the importance of safeguarding the PII entrusted to it by Plaintiff and Class members, and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on Plaintiff and Class Members as a result of a breach.

97. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

Defendant Failed to Follow FTC Guidelines

98. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. Thus, the FTC issued numerous guidelines identifying best data security practices that businesses—like Defendant—should use to protect against unlawful data exposure.

99. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*. There, the FTC set guidelines for what data security principles and practices businesses must use.[52] The FTC declared that, *inter alia*, businesses must:

a. protect the personal customer information that they keep;

---

[50] *See* Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack*, SECURITY MAGAZINE (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack (last visited Sept. 11, 2023).

[51] *See* https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/ (last visited April 8, 2024).

[52] *Protecting Personal Information: A Guide for Business,* FEDERAL TRADE COMMISSION (Oct. 2016) https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

100. The guidelines also recommend that businesses watch for the transmission of large amounts of data out of the system—and then have a response plan ready for such a breach.

101. Furthermore, the FTC explains that companies must:

a. not maintain information longer than is needed to authorize a transaction;

b. limit access to sensitive data;

c. require complex passwords to be used on networks;

d. use industry-tested methods for security;

e. monitor for suspicious activity on the network; and

f. verify that third-party service providers use reasonable security measures.

102. The FTC brings enforcement actions against businesses for failing to protect customer data adequately and reasonably. Thus, the FTC treats the failure—to use reasonable and appropriate measures to protect against unauthorized access to confidential consumer data—as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

103. In short, Defendant's failure to use reasonable and appropriate measures to protect against unauthorized access to its current and former employees' and/or customers' data constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Failed to Follow Industry Standards

104. Several best practices have been identified that—at a *minimum*—should be implemented by businesses like Defendant. These industry standards include: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption (making data unreadable without a key); multi-factor authentication; backup data; and limiting which employees can access sensitive data.

105. Other industry standard best practices include: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

106. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

107. These frameworks are applicable and accepted industry standards. And by failing to comply with these accepted standards, Defendant opened the door to the criminals—thereby causing the Data Breach.

Defendant Violated HIPAA

108. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep patients' medical information safe. HIPAA compliance provisions, commonly

known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information.[53]

109. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII/PHI and PHI is properly maintained.[54]

110. The Data Breach itself resulted from a combination of inadequacies showing Defendant failed to comply with safeguards mandated by HIPAA. Defendant's security failures include, but are not limited to:

a. failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. § 164.306(a)(1);

b. failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

c. failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

---

[53] HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, *inter alia*: names, addresses, any dates including dates of birth, Social Security numbers, and medical record numbers.

[54] *See* 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards).

d. failing to ensure compliance with HIPAA security standards by Defendant's workforce in violation of 45 C.F.R. § 164.306(a)(4);

e. failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

f. failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);

g. failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

h. failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

i. failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

111. Simply put, the Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations.

CLASS ACTION ALLEGATIONS

112. Plaintiffs bring this class action under Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), individually and on behalf of all members of the following class:

> All individuals residing in the United States whose PII/PHI was compromised in the Data Breach discovered by Nautic in 2023, including all those individuals who received notice of the breach.

113. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

114. Plaintiffs reserve the right to amend the class definition.

115. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on class-wide bases using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

116. Ascertainability. All members of the proposed Class are readily ascertainable from information in Defendant's custody and control. After all, Defendant already identified some individuals and sent them data breach notices.

117. Numerosity. The Class members are so numerous that joinder of all Class members is impracticable. Upon information and belief, the proposed Class includes at least 7,870 members.

118. Typicality. Plaintiffs' claims are typical of Class members' claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

119. Adequacy. Plaintiffs will fairly and adequately protect the proposed Class's common interests. Her interests do not conflict with Class members' interests. And Plaintiffs have

retained counsel—including lead counsel—that is experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf.

120. Commonality and Predominance. Plaintiffs' and the Class's claims raise predominantly common fact and legal questions—which predominate over any questions affecting individual Class members—for which a class wide proceeding can answer for all Class members. In fact, a class wide proceeding is necessary to answer the following questions:

a. if Defendant had a duty to use reasonable care in safeguarding Plaintiffs' and the Class's PII/PHI;

b. if Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. if Defendant were negligent in maintaining, protecting, and securing PII/PHI;

d. if Defendant breached contract promises to safeguard Plaintiffs and the Class's PII/PHI;

e. if Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

f. if Defendant's Breach Notice was reasonable;

g. if the Data Breach caused Plaintiffs and the Class injuries;

h. what the proper damages measure is; and

i. if Plaintiffs and the Class are entitled to damages, treble damages, and or injunctive relief.

121. Superiority. A class action will provide substantial benefits and is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class members are relatively small compared to the burden and expense that individual litigation against Defendant would require. Thus, it would be practically impossible for Class members, on an individual basis, to obtain effective redress for their injuries. Not only would individualized litigation increase the delay and expense to all parties and the courts, but individualized litigation would also create the danger of inconsistent or contradictory judgments arising from the same set of facts. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, ensures economies of scale, provides comprehensive supervision by a single court, and presents no unusual management difficulties.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiffs and the Class)

122. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

123. Plaintiffs and the Class (or their third-party agents) entrusted their PII/PHI to Defendant on the premise and with the understanding that Defendant would safeguard their PII/PHI, use their PII/PHI for business purposes only, and/or not disclose their PII/PHI to unauthorized third parties.

124. Defendant owed a duty of care to Plaintiffs and Class members because it was foreseeable that Defendant's failure—to use adequate data security in accordance with industry standards for data security—would compromise their PII/PHI in a data breach. And here, that foreseeable danger came to pass.

125. Defendant has full knowledge of the sensitivity of the PII/PHI and the types of harm that Plaintiffs and the Class could and would suffer if their PII/PHI was wrongfully disclosed.

126. Defendant owed these duties to Plaintiffs and Class members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security practices. After all, Defendant actively sought and obtained Plaintiffs' and Class members' PII/PHI.

127. Defendant owed—to Plaintiff and Class members—at least the following duties to:

a. exercise reasonable care in handling and using the PII/PHI in its care and custody;

b. implement industry-standard security procedures sufficient to reasonably protect the information from a data breach, theft, and unauthorized;

c. promptly detect attempts at unauthorized access;

d. notify Plaintiffs and Class members within a reasonable timeframe of any breach to the security of their PII/PHI.

128. Thus, Defendant owed a duty to timely and accurately disclose to Plaintiffs and Class members the scope, nature, and occurrence of the Data Breach. After all, this duty is required and necessary for Plaintiffs and Class members to take appropriate measures to protect their PII/PHI, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

129. Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII/PHI it was no longer required to retain under applicable regulations.

130. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII/PHI of Plaintiffs and the Class involved an

unreasonable risk of harm to Plaintiffs and the Class, even if the harm occurred through the criminal acts of a third party.

131. Defendant's duty to use reasonable security measures arose because of the special relationship that existed between Defendant and Plaintiffs and the Class. That special relationship arose because Plaintiffs and the Class (or their third-party agents) entrusted Defendant with their confidential PII/PHI, a necessary part of obtaining services from Defendant.

132. Under the FTC Act, 15 U.S.C. § 45, Defendant had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiffs and Class members' PII/PHI.

133. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect the PII/PHI entrusted to it. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiffs and the Class members' sensitive PII/PHI.

134. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect PII/PHI and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII/PHI Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

135. Similarly, under HIPAA, Defendant had a duty to follow HIPAA standards for privacy and security practices—as to protect Plaintiffs' and Class members' PHI.

136. Defendant violated its duty under HIPAA by failing to use reasonable measures to protect its PHI and by not complying with applicable regulations detailed *supra*. Here too,

Defendant's conduct was particularly unreasonable given the nature and amount of PHI that Defendant collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

137. The risk that unauthorized persons would attempt to gain access to the PII/PHI and misuse it was foreseeable. Given that Defendant hold vast amounts of PII/PHI, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII/PHI —whether by malware or otherwise.

138. PII/PHI is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII/PHI of Plaintiffs and Class members' and the importance of exercising reasonable care in handling it.

139. Defendant improperly and inadequately safeguarded the PII/PHI of Plaintiffs and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

140. Defendant breached these duties as evidenced by the Data Breach.

141. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs' and Class members' PII/PHI by:

a. disclosing and providing access to this information to third parties and

b. failing to properly supervise both the way the PII/PHI was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

142. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal

information and PII/PHI of Plaintiffs and Class members which actually and proximately caused the Data Breach and Plaintiffs' and Class members' injury.

143. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and Class members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiffs' and Class members' injuries-in-fact.

144. Defendant has admitted that the PII/PHI of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

145. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiffs and Class members have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

146. And, on information and belief, Plaintiffs' PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

147. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiffs and Class members actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII/PHI by criminals, improper disclosure of their PII/PHI, lost benefit of their bargain, lost value of their PII/PHI, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

SECOND CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiffs and the Class)

148. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

149. Plaintiffs and Class members either directly contracted with Defendant or Plaintiffs and Class members were the third-party beneficiaries of contracts with Defendant.

150. Plaintiffs and Class members (or their third-party agents) were required to provide their PII/PHI to Defendant as a condition of receiving services and/or employment provided by Defendant. Plaintiffs and Class members (or their third-party agents) provided their PII/PHI to Defendant or its third-party agents in exchange for Defendant's services and/or employment.

151. The contracts entered into by Plaintiffs' and Class members' agents, were made for the direct benefit of Plaintiffs and the Class.

152. Plaintiffs and Class members (or their third-party agents) reasonably understood that a portion of the funds they paid to Defendant (and/or derived from their employment) would be used to pay for adequate cybersecurity measures.

153. Plaintiffs and Class members (or their third-party agents) reasonably understood that Defendant would use adequate cybersecurity measures to protect the PII/PHI that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

154. Plaintiffs and the Class members (or their third-party agents) accepted Defendant's offers by disclosing their PII/PHI to Defendant or its third-party agents in exchange for services and/or employment.

155. In turn, and through internal policies, Defendant agreed to protect and not disclose the PII/PHI to unauthorized persons.

156. In its Privacy Policy, Defendant represented that they had a legal duty to protect Plaintiffs' and Class Member's PII/PHI.

157. Implicit in the parties' agreement was that Defendant would provide Plaintiffs and Class members (or their third-party agents) with prompt and adequate notice of all unauthorized access and/or theft of their PII/PHI.

158. After all, Plaintiffs and Class members (or their third-party agents) would not have entrusted their PII/PHI to Defendant (or their third-party agents) in the absence of such an agreement with Defendant.

159. Plaintiffs and the Class (or their third-party agents) fully performed their obligations under the implied contracts with Defendant.

160. The covenant of good faith and fair dealing is an element of every contract. Thus, parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—and not merely the letter—of the bargain. In short, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

161. Subterfuge and evasion violate the duty of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or consist of inaction. And fair dealing may require more than honesty.

162. Defendant materially breached the contracts it entered with Plaintiffs and Class members (or their third-party agents) by:

a. failing to safeguard their information;

b. failing to notify them promptly of the intrusion into its computer systems that compromised such information.

c. failing to comply with industry standards;

d. failing to comply with the legal obligations necessarily incorporated into the agreements; and

e. failing to ensure the confidentiality and integrity of the electronic PII/PHI that Defendant created, received, maintained, and transmitted.

163. In these and other ways, Defendant violated its duty of good faith and fair dealing.

164. Defendant's material breaches were the direct and proximate cause of Plaintiffs' and Class members' injuries (as detailed *supra*).

165. And, on information and belief, Plaintiffs' PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

166. Plaintiffs and Class members (or their third-party agents) performed as required under the relevant agreements, or such performance was waived by Defendant's conduct.

THIRD CAUSE OF ACTION
Invasion of Privacy
R.I. Gen. Laws § 9-1-28.1
(On Behalf of Plaintiffs and the Class)

167. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

168. R.I. Gen. Laws § 9-1-28.1 establishes individuals' right to privacy.

169. Defendant violated § 9-1-28.1(a)(1) by abrogating Class Members' "right to be secure from unreasonable intrusion upon one's physical solitude or seclusion."

170. Also, Defendant violated § 9-1-28.1(a)(3) by abrogating Class Members' "right to be secure from unreasonable publicity given to one's private life."

171. Plaintiffs and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential PII/PHI and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

172. Defendant owed a duty to its current and former employees and/or customers, including Plaintiffs and the Class, to keep this information confidential.

173. The unauthorized acquisition (i.e., theft) by a third party of Plaintiffs and Class members' PII/PHI is highly offensive to a reasonable person.

174. The intrusion was into a place or thing which was private and entitled to be private. Plaintiffs and the Class (or their third-party agents) disclosed their sensitive and confidential information to Defendant, but did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiffs and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

175. The Data Breach constitutes an intentional interference with Plaintiffs' and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

176. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

177. Defendant acted with a knowing state of mind when it failed to notify Plaintiffs and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

178. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiffs and the Class.

179. As a proximate result of Defendant's acts and omissions, the private and sensitive PII/PHI of Plaintiffs and the Class were stolen by a third party and is now available for disclosure

and redisclosure without authorization, causing Plaintiffs and the Class to suffer damages (as detailed *supra*).

180. And, on information and belief, Plaintiffs' PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

181. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class since their PII/PHI are still maintained by Defendant with their inadequate cybersecurity system and policies.

182. Plaintiffs and the Class have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the PII/PHI of Plaintiffs and the Class.

183. In addition to injunctive relief, Plaintiffs, on behalf of themselves and the other Class members, also seek compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

FOURTH CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

184. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

185. This claim is pleaded in the alternative to the breach of implied contract claim.

186. Plaintiffs and Class members (or their third-party agents) conferred a benefit upon Defendant. After all, Defendant benefitted from using their PII/PHI, money, and/or employment to provide services and/or facilitate employment.

187. Defendant appreciated or had knowledge of the benefits it received from Plaintiffs and Class members (or their third-party agents).

188. Plaintiffs and Class members (or their third-party agents) reasonably understood that Defendant would use adequate cybersecurity measures to protect the PII/PHI that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

189. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs' and Class members' PII/PHI.

190. Instead of providing a reasonable level of security, or retention policies, that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiffs and Class members by utilizing cheaper, ineffective security measures. Plaintiffs and Class members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

191. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiffs' and Class members' PII/PHI, money, and/or employment because Defendant failed to adequately protect their PII/PHI.

192. Plaintiffs and Class members have no adequate remedy at law.

193. Defendant should be compelled to disgorge into a common fund—for the benefit of Plaintiffs and Class members—all unlawful or inequitable proceeds that it received because of its misconduct.

FIFTH CAUSE OF ACTION
Violation of the Rhode Island Deceptive Trade Practices Act
R.I. Gen. Laws § 6-13.1 *et seq*.
(On Behalf of Plaintiffs and the Class)

194. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

195. Under R.I. Gen. Laws § 6-13.1-2, "[u]nfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are declared unlawful."

196. Defendant engaged in unfair or deceptive acts or practices, by *inter alia*:

a. failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Class members' PII/PHI, which was a direct and proximate cause of the Data Breach;

b. failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class members' PII/PHI, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq*., which was a direct and proximate cause of the Data Breach;

d. omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class members' PII/PHI; and

e. omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class members' PII/PHI, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq*.

197. Defendant's omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of their PII/PHI.

198. Defendant intended to mislead Plaintiffs and Class members and induce them to rely on its omissions.

199. Had Defendant disclosed to Plaintiffs and Class members (or their third-party agents) that its data systems were not secure—and thus vulnerable to attack—Defendant would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Defendant accepted the PII/PHI that Plaintiffs and Class members (or their third-party agents) entrusted to it while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiffs and Class members acted reasonably in relying on Defendant's omissions, the truth of which they could not have discovered through reasonable investigation.

200. Defendant acted intentionally, knowingly, maliciously, and recklessly disregarded Plaintiffs' and Class members' rights.

201. As a direct and proximate result of Defendant's unfair and deceptive acts and practices, Plaintiffs and Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII/PHI.

202. And, on information and belief, Plaintiffs' PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

203. Plaintiffs and Class members seek all monetary and non-monetary relief allowed by law.

SIXTH CAUSE OF ACTION
Declaratory Judgment
(On Behalf of Plaintiffs and the Class)

204. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

205. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. The Court has broad authority to restrain acts, such as those alleged herein, which are tortious and unlawful.

206. In the fallout of the Data Breach, an actual controversy has arisen about Defendant's various duties to use reasonable data security. On information and belief, Plaintiffs allege that Defendant's actions were—and *still* are—inadequate and unreasonable. And Plaintiffs and Class members continue to suffer injury from the ongoing threat of fraud and identity theft.

207. Given its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owed—and continues to owe—a legal duty to use reasonable data security to secure the data entrusted to it;

b. Defendant has a duty to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;

c. Defendant breached, and continues to breach, its duties by failing to use reasonable measures to the data entrusted to it; and

d. Defendant breaches of its duties caused—and continues to cause—injuries to Plaintiffs and Class members.

208. The Court should also issue corresponding injunctive relief requiring Defendant to use adequate security consistent with industry standards to protect the data entrusted to it.

209. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury and lack an adequate legal remedy if Defendant experiences a second data breach.

210. And if a second breach occurs, Plaintiffs and the Class will lack an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages—while warranted for out-of-pocket damages and other legally quantifiable and provable damages—cannot cover the full extent of Plaintiffs and Class members' injuries.

211. If an injunction is not issued, the resulting hardship to Plaintiffs and Class members far exceeds the minimal hardship that Defendant could experience if an injunction is issued.

212. An injunction would benefit the public by preventing another data breach—thus preventing further injuries to Plaintiffs, Class members, and the public at large.

PRAYER FOR RELIEF

Plaintiffs and Class members respectfully request judgment against Defendant and that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiffs and the proposed Class, appointing Plaintiffs as class representatives, and appointing their counsel to represent the Class;

B. Awarding declaratory and other equitable relief as necessary to protect the interests of Plaintiffs and the Class;

C. Awarding injunctive relief as necessary to protect the interests of Plaintiffs and the Class;

D. Enjoining Defendant from further unfair and/or deceptive practices;

E. Awarding Plaintiffs and the Class damages including applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiffs and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiffs and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting other relief that this Court finds appropriate.

DEMAND FOR JURY TRIAL

Plaintiffs demand a jury trial for all claims so triable.

Date: May 3, 2024

Respectfully submitted,

/s/ David K. Lietz
David K. Lietz (*pro hac vice*)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
5335 Wisconsin Avenue NW, Suite 440
Washington, D.C. 20015-2052
Telephone: (866) 252-0878
Facsimile: (202) 686-2877
dlietz@milberg.com

TURKE & STRAUSS LLP
Samuel J. Strauss
Raina Borrelli
613 Williamson Street, Suite 201
Madison, Wisconsin 53703
Telephone: (608) 237-1775
Facsimile: (608) 509-4423
sam@turkestrauss.com
raina@turkestrauss.com

Vincent L. Greene
MOTLEY RICE LLC
40 Westminster St., 5th Floor
Providence, RI 02903
Ph: (401) 457-7730
Fax.: (401) 457-7708
vgreene@motleyrice.com

Attorneys for Plaintiffs and Proposed Class